Scambaiting on the Spectrum of Digilantism[1]

Abstract

Digilantism is punishing online exposure of supposed wrongdoing. Paedophile hunting is one example, and is open to many of the classical objections to vigilantism. But it lies on a spectrum that contains many kinds of digilantism. Scambaiting is among the other kinds. It consists of attracting online approaches from perpetrators of different kinds of online advance fee fraud. Characteristically, it takes the form of protracted email exchanges between scammers and scambaiters. These exchanges are mainly down -to-earth and occasionally testy conversations about the details of fictitious money transfers or involved explanations of delays in payment. They succeed in their purpose if they waste a lot of their targets' time. But they can also be pursued as a sort of comic art form. Scambaiting exchanges seem often, but not always, to be relatively harmless. They therefore help to make intelligible a region of morally permissible digilantism on the spectrum of digilantism. Not that scambaiters never go too far, but their typical weapons inflict and risk inflicting far less harm than those of other digilantes and there are actual scambaiting norms that are chosen because of their relative harmlessness.

I

Digilantism is punishing exposure online of supposed wrongdoing. Its targets are the agents of that wrongdoing: individuals as well as groups, states and corporations.[2] Digilantism

involves, besides those who identify the supposed wrongdoing and the actions condemned, an online audience who are expected to agree that norms they respect have been violated. The norms violated are sometimes expressed in criminal laws but need not be: digilantism can and often does target *sub*criminal activity e.g. the use of sexist language or sexist jokes.[3]. The audiences for digilantism are sometimes recruited from pre-existing online subgroups with identifiable positions on such things as animal cruelty, feminism, or gun control. Appeals to these audiences can sometimes produce a "pile on" – co-ordinated online abuse, deprecation or criticism--directed at a single target. Participants in pile-ons often operate under pseudonyms. Digilantism thus overlaps with "trolling" or unco-ordinated online abuse by anonymous individuals targeting other individuals.[4] Pile-ons and trolling can produce threats – sometimes carried out – of physical violence as well as psychological harm in the form of humiliation, self-hate and depression in victims.

Although all forms of digilantism raise moral questions, I shall focus on *narrowly-defined digilantism:* retaliation organized on the internet for acts that are formally criminalized where they take place, and that are assumed by digilantes to go unpunished by the relevant authorities. This brings digilantism closer to one definition of offline vigilantism: namely, extra-legal "punishment" – hard treatment – meted out to local people supposedly responsible for acts formally criminalized or otherwise forbidden in that community or jurisdiction. Narrowly defined digilantism is of philosophical interest not only because vigilantism is, but because direct citizen participation in crime control is increasingly tolerated in liberal states:[5] digilantism may be seen, by digilantes and others, as an admirable form of active citizenship that also includes neighbourhood watch schemes and crime reporting hotlines.[6]

An example of narrowly defined digilantism that is sometimes officially or unofficially condoned by the authorities in liberal states is paedophile-hunting. Paedophile-hunting is sometimes represented as an "activist" response to a genuine threat to children from adults grooming them online for sex. In some jurisdictions the volume of grooming is said to be too great to be controlled by the police:[7] digilantes can think of themselves as taking up the slack. They pose online as children in online chatrooms known to be used by groomers and in effect offer their personas as bait. Paedophiles who take the bait and eventually arrive at an agreed offline location expecting to have sex with a child, are met and verbally chastised by digilantes, and videos of the encounters are posted online to shame them. At the same time or subsequently, local police are sometimes invited to make an arrest, and the digilantes sometimes hand over their chatlogs as evidence for a prosecution. Co-operation with police is not always a feature of paedophile-hunting activity, however. Sometimes the digilantes aim at online shaming alone or at online shaming combined with chastisement. In some illiberal jurisdictions, notably Russia, paedophiles are often confronted very violently, and paedophilia is conflated with homosexuality.[8]

As will emerge, paedophile-hunting is open to many of the classical objections to vigilantism. But it is only one form of digilantism in a spectrum that contains many other kinds of activity. Scambaiting is among the other kinds. It consists of attracting online approaches from perpetrators of different kinds of advance fee fraud. Probably the best known of these is the 419 scam, named after the section of Nigerian legislation outlawing it. In a 419 scam someone with an email address is asked to receive a large amount of money from abroad into his or her bank account, a significant share of which they can supposedly

keep. The few who show interest are required by fraudsters to give away bank account details and to make many advance payments --supposedly to facilitate the release of the very large sum, which eventually turns out not to exist. Scambaiters try to attract the characteristic online pitches of scammers and then proceed to waste the fraudsters' time, sometimes sending them to remote locations to await payments that never arrive.

Scambaiting sometimes produces identifying information, including images of scammers, which may or may not be useful in a prosecution. Characteristically, however, it takes the form of protracted email exchanges with scammers. These exchanges are mainly down -to-earth and occasionally testy conversations about the details of fictitious money transfers or involved explanations of delays in payment. They succeed in their purpose if they waste a lot of their targets' time. But, as we will see, they can also be pursued as a sort of comic art form. Whatever their usefulness to the local police – and that might be limited by the de facto impunity of scammers in their far away jurisdictions – scambaiting exchanges seem often, but not always, to be relatively harmless. They therefore help to make intelligible a region of morally permissible digilantism on the spectrum of digilantism. Not that scambaiters never go too far. But their typical weapons inflict and risk inflicting far less harm than those of other digilantes, and there are actual scambaiting norms that have been chosen *because* of their relative harmlessness.

The rest of this paper is divided into three parts. I first run through some general objections to vigilantism and argue that they apply to some kinds of digilantism as well. In section 2, I show how one widely practiced form of narrowly defined digilantism already mentioned– paedophile-hunting-- is open to those objections. I then try to explain how scambaiting can

be different. I do not claim that there is only one form of scambaiting, but I identify examples of actual scambaiting that are ethically scrupulous in the sense that that they correctly reject certain means of scamming the scammers as wrong. I also identify goals of scambaiters that co-exist with and constrain the goal of punishing scammers. I then entertain some objections drawn from the cultural and economic differences between scammers and scam victims that may seem to excuse some of the harm of scamming, and that may count against some kinds of scambaiting. I try to rebut these objections.

II

Digilantism – or online vigilantism – has been exposed to very little systematic definitional work,[9] and there is little or no literature connecting it at any length with vigilantism. Much previous work on digilantism is connected with hate speech, including 'trolling'. In a series of papers, Jane[10] has taken up misogynist hate speech and digilantist responses to hate speech, but often in contexts where the activity that inspires digilantism is subcriminal, and where digilantism consists of "calling out" – calling critical attention to – hate speech and its perpetrators. There is a considerable general literature on online hate speech and shaming.[11] A growing legal literature has been reviewed by Laidlaw in a recent paper connecting online shaming to violations of privacy.[12] Philosophical literature on online hate speech and other objectionable content is sparse but includes Levmore and Nussbaum.[13]

In the recent media studies literature, digitlantism is associated with the "weaponization of visibility".[14] The "weaponization" emerges midway in a three-stage process. First, alleged

wrongdoing of various kinds is publicized online, often in the form of videos; next, the online audience is prompted to collaborate in identifying the culprits and "punishing" them either through online abuse or outright violence. Third, the online audience is kept abreast of developments, including identifications of culprits, online and offline action against them, pleas for additional support etc. This pattern is certainly present in many kinds of digilantism, but, as we shall see, scambaiting does not conform to it, and neither does some hacktivist activity, notably Distributed Denial of Service (DDoS) attacks. Sometimes, as in scambaiting, digilantism seems to consist of weaponized humour and inconvenience rather than abuse.

Many of the objections to vigilantism [15] are close to the surface in the definition "extra-legal punishment of local people supposedly responsible for criminalized acts." First, vigilantes can be mistaken about the occurrence of the criminalized act. Even where they are not mistaken about that, they can misidentify culprits. Second, they can mete out much harsher treatment than liberal legislation threatens for violators. Often, vigilantes inflict extreme physical violence, some of it lethal. Third, vigilantes have no obvious mechanisms for registering excuses or justifications for the acts they punish. Fourth, vigilantes do not necessarily deal with all local culprits, or with relevantly similar culprits, in similar ways. In short, the hard treatment dispensed by vigilantes can be inconsistently applied, disproportionately severe, and directed at the innocent. Objections to vigilantism serve as reasons for supporting impersonal, liberal institutions for legislation, law enforcement and punishment that criminalize vigilantism.

Arguably, there is a history of vigilantism in America going back as far as the 1770s and running up until the present day (Juliano, 2012). It is mainly associated, however, with a period in the 19th century in which people with a complaint about a crime on the frontier – the "wild West" – relied on relatively few local law-officers and hastily deputized volunteers to apprehend suspects (Obert, 2018). Later these were supplemented with private detective agencies, such as Pinkerton's. In the UK in the 19th century, female vigilante action targeted prostitution in some areas (Bland, 2011). Recent vigilante action on a relatively large scale occurred in 2011 in response to looting during riots in the main English cities. In some cases during this period, vigilantes were seen as engaging in self-defence rather than informal law enforcement, because they took the law into their own hands to defend their own property. Finally, in the very recent past in the USA a new kind of vigilante has been invented, based on comic-book superheroes. Private citizens, some with martial arts skills, take it upon themselves to protect the helpless, usually in high-crime urban areas. In very well-known cases, such figures impersonate the comic book characters they are named after by dressing up in the relevant costumes (Fezzani, 2016). Vigilantes of both these kinds operate publicly in the communities they assist, and have particular local territories.

By contrast, digilantes may be located thousands of miles from targets they have never met, and they may contribute anonymously to psychological hard treatment without themselves ever being threatened. The effect of traditional vigilante action can be to drive supposed offenders out of a community and to a place where they are not known. The effects of digilante action, on the other hand, are sometimes impossible to escape simply by changing one's locality, because of the wide reach of the internet, and the huge importance many people attach to online personas they cultivate on social media sites. Escape from

digilantes may require nothing less than closing one's social media accounts, changing one's name and hiding one's former identity.

These distinctive features notwithstanding, many objections against vigilantism are also objections against narrowly defined digilantism. Digilantes can incorrectly claim that a legal offence or wrongdoing has been committed. They can misidentify culprits. They can mete out much harsher comment for violations of norms than mainstream critics of the same behavior would judge to be appropriate. They have no obvious mechanisms for registering excuses or justifications for acts on the part of those attacked. Digilantes do not necessarily deal with many culprits, or with relevantly similar culprits, in similar ways. In short, the hard treatment dispensed by digilantes can be, like traditional vigilante violence, inconsistent, disproportionate and directed at the innocent.

III

To illustrate kinds of narrowly-defined digilantism that attract many of the same objections as traditional vigilantism, we turn in this section to paedophile-hunting. Paedophile-hunters aim at shaming exposure of online groomers. In the standard case, middle-aged, male online groomers believe that they are in chatroom or SMS contact with girls entering their teens. Chatroom discussion is carefully orchestrated on both sides. The groomers often pose as teenagers and ask their targets intermittently about the current whereabouts of adults or parents. They often adopt teenage texting conventions. They steer the discussion gradually toward sexual topics and, eventually, suggest a meeting for sex. The challenge for

paedophile hunters is to create a credible child persona who shows interest in sex when it is proposed by the groomer, but who does not take the initiative. Paedophile hunters use various methods to persuade groomers to be quite explicit about their interests and intentions. If a meeting for sex *is* proposed, at least in the UK,[16] paedophile hunters often go equipped with video cameras to the appointed place and reveal themselves as the source of the child personas whom the groomers have come to meet.

When confronted by hunters, the groomers are sometimes contrite, sometimes in a panic, and sometimes calm but eager to get away. The confrontation can take place in a location with many passers-by, so that some shaming is accomplished even before a video is posted. Episodes along these lines can sometimes run the risk of violence and often involve degrees of coercion. The hunters may detain the groomer until police they have contacted arrive. Or they may do nothing to obstruct a groomer but follow along with cameras and questions in the manner of investigative journalists. In those cases, they will have often taken down the groomer's car number, and of course they have a full chatlog record to post on a website and give to the police. Sometimes they bypass the police, posting identifying details of the groomer to a general audience and leaving it up to them to choose appropriate retaliation. Other hunters pass on their evidence to police immediately after a filmed confrontation and take no further action themselves against the groomers. The UK group Dark Justice[17] adopts low-key tactics of this kind.

In the UK, lawyers acting for paedophiles prosecuted as a result of digilante action have complained in court of taint to the legal process from a reliance on digilante evidence. The

same lawyers claimed in 2017 that paedophile hunters should be subject to the processes of applying for warrants to pose as children that the police are subject to in their online sting operations. The judge in the relevant case rejected these claims, upholding the right of digilantes to go about their work of identifying groomers as relatively unfettered private citizens rather than public officials.[18] On the other hand, guidance issued as late as 2019 by the Crown Prosecution Service makes it clear not only that paedophile hunting is unnecessary and undesirable, but that paedophile hunters are liable to be prosecuted themselves for offences such as making indecent images, among others.[19] In general, vigilante activity is officially considered unhelpful in England and Wales, even when it is intended to prevent crimes against children.

Perverted Justice (subsequently 'PJ') is a US paedophile-hunting group established in 2002 and is perhaps the best known of its type globally. Volunteers create the personas of children in chatrooms, orchestrate online conversations to elicit identifying contact details from groomers, and hand over chatlog records to police local to the groomers. Groomers are normally prosecuted, and, after conviction, their chatlogs are posted on the PJ website. In at least one case of non-prosecution, a chatlog was posted anyway: PJ identified a groomer who was forthcoming about both his age and occupation (School Principal) to a chatroom persona he believed was a 13-year old girl.[20] The man lost his job.

PJ rose to prominence in the USA through a link with a national broadcaster between 2004 and 2007. The NBC network program *To Catch a Predator* broadcast confrontations between groomers and the show's host, Chris Hansen, to a large national audience. NBC rented houses in various locations to serve as meeting places and controlled environments.

Groomers would be told by their child chatlog partners that these were suitable places to meet. On arrival the groomers would be greeted by an actress impersonating the relevant online child persona. The preliminary meeting (not known by the groomers to be televised) would establish continuity between the intentions expressed in the online chatlog and the groomers' intentions in the face-to-face meeting. Then Hansen would appear, disconcerting the groomers and delving deeper into their plans. The groomers were free to leave the interview with Hansen at any time.

In the earliest series, groomers left without any immediate action being taken against them, though chatlogs and identifying evidence were passed to police. Later, however, the NBC programme format changed: as soon as groomers left what we might call the "show house", they were filmed being arrested. Later, also on camera, they were questioned by police. Even their court appearances for bail were broadcast.

Before its collaboration with NBC, PJ operated differently. One of its co-founders, the improbably named Fred Fencepost, invited unsuspecting online groomers to his own home and treated them to shaming confrontations on the spot.[21] These and other aggressive tactics led to falling out between Fencepost and the other co-founder of PJ, Xavier Van Erck. The result appears to have been a policy of less personal confrontation on the part of those creating child personas, and more posting of chatlogs to a disapproving internet audience. In its early days, PJ simply published chatlogs at the point at which groomers sexualized conversations. Visitors to its online forums might then identify and harass groomers or try to inform their family members to shame them. Later, PJ would give its chatlogs straight to

local police, and invite them to follow up. Convictions arising from this co-operation with the authorities were (and continue to be) advertised by PJ as evidence of its own impact.

In order to indicate what might be morally objectionable about PJ, it is worth contrasting its activity with two different kinds of anti-paedophile operation on the part of *police.* (1) Police are alerted to the online grooming of a child by e.g. the child's parents. Police then try to take over the online conversation by using the child's linguistic mannerisms. When the groomer suggests a meeting for sex, they arrest and prosecute the groomer. This is the form that preventive policing of online child abuse sometimes takes in the UK.[22] Alternatively, (2) police construct the persona of a child on an online chatroom to attract a groomer, conduct a prolonged internet conversation with someone who takes the bait, and then, when he suggests a meeting, go to the appointed place and make an arrest.

It seems clear that (1) is morally superior to (2). The reason is that in (1) a real child is protected from harm, and the police have had no role in engaging the interest of the groomer. In (2) no child is at risk, the persona being invented by the police, and it is at least *possible* in some cases that *but* for the police invention of the persona the groomer would not have contacted a child persona. The fact that (1) is morally superior to (2) does not mean that (2) is impermissible. It is permissible to the extent that the child persona does nothing to initiate the movement from sexualized conversation to meeting and does nothing to begin the sexualization of the conversation. Even when those conditions are met, there is a residue of risk of immorality. For maintaining a sexualized conversation after it has been started by the groomer is morally challenging: the groomer will often try to elicit expressions of enthusiasm or interest in sex from the child persona, and it is better

morally if the persona's contributions to the conversation are minimal. This is not a point about steering clear of the legal threshold for entrapment, but rather about the basis for entrapment being a concern at all: namely, that people who enforce the law should not *add* to anyone's appetite for breaking it. The police may permit the appetite to take its course, but should not stoke it up, so to speak.

To my knowledge, the practice of PJ has never followed the pattern of (1): it runs along the lines of (2). But there are morally important differences between the police version of (2) and the PJ-version of (2) as described in the few sources that describe it. The police in technologically sophisticated jurisdictions e.g. the UK, are usually able[23] quickly to trace the IP address of the groomer and then identify him. They are also able to establish at an early stage whether the groomer has a criminal record, and, in particular, a previous history of sexual offences. This information will affect the tactics chosen for arrest and follow-up work on other online activity of the groomer. In the UK, the police concentrate their efforts on groomers of personas advertised as 13 years old or younger, on middle-aged groomers who misrepresent themselves as teenagers, and groomers who do not merely indulge in sexualized conversation but try to arrange meetings for sex. This is because the relevant piece of legislation in England and Wales up to 2017, namely Section 15 of the Sexual Offences Act (2003), criminalized only grooming that leads to a meeting.

The police know that the chatlogs they compile will function as the key evidence in a trial on a Section 15 offence; in particular, they know that the record must survive challenges from lawyers alleging entrapment. Chatlog entries appearing to show that a police-constructed persona initiated talk of a meeting, or initiated sexualized conversation, or offered sexual

favours, are relevant to such challenges. Police are trained to keep their persona's conversations within the law. They would never publish chatlogs, even after conviction, and, though arrests and post-arrest police interviews for Section 15 offences are sometimes filmed and included in TV documentaries about paedophiles, the names of groomers are only broadcast after conviction.

The methods of PJ in conjunction with the NBC program 'To Catch a Predator' (hereafter TCP) have been much less constrained by legal scruples both in the online conversation process and in the process leading to meeting and confronting the groomers. Or at least, that is what relevant journalism indicates. The American magazine *Rolling Stone* published an article about PJ methods and personnel in July 2007. It reported on a TCP sting operation in New Jersey in 2007 in which the threshold for entrapment seemed to be reached repeatedly in conversations with groomers who were on their way to the relevant show-house.[24]

Assuming that the journalism, is accurate, what does it show about the PJ-TCP version of approach (2) to groomers? First, that the demands of television can make for an objectionable production line of groomer meetings, the meetings themselves being prompted by an objectionably pro-active offer of sex augmented by the telephone exhortations of the online persona. The inattention to age-difference suggests that in the PJ-TCP view, the chatline and offline behavior of very young men with no criminal record is morally no different to that of the chatlog participant who is much older, more experienced, and a repeat sex-offender. The criteria of police in England and Wales for concentrating

their type (2) activity on 13 year-old victims of middle-aged groomers seems, by comparison, closer to being proportionate.

More fundamentally, there are questions about the training and conscientiousness of those conducting chatline conversations with groomers. *Are* they skilled in the fine art of both maintaining the interest of groomers and avoiding entrapment? As PJ goals have evolved from shaming online exposure of groomers to convictions of groomers on the basis of PJ chatlogs, the need to avoid entrapment has become more acute. The new goal also raises the question of who the compilers of the chatlogs are, how they have been chosen, and whether they need to be formally deputized by the police when co-operation leads to prosecutions. More specifically, do the PJ chatroom personnel have clean criminal records? Is there anything to stop them talking about or even threatening the groomers they interact with? Then there are the offences that can be provoked when convicted paedophiles are identified for audiences keen to retaliate physically against them or their families.

We may distinguish between PJ-type activity where the aim is to collect evidence for criminal prosecutions, and PJ-type activity where the aim is to inflict punishing exposure on those whose grooming on chatlogs has been documented. The latter seems to be typical of anti-paedophile activity internationally, and not just PJ. In both its early and late forms, PJ activists have sought to publicize the identities of online groomers in their localities. The moral risks of this practice are obvious. People who are identified can happen to have the same names as perfectly innocent people who also live there, and who may be mistaken for groomers. It is quite possible that people who are only guilty of online grooming will be taken to be guilty of much more serious offences, like child rape. Perhaps groomers will be

targeted for the kinds of beatings and worse sometimes reserved for the rapists. These are dangers of releasing identifying information to online forums. In the case of PJ, there is the further unnecessary flourish of publicizing a list of the "10 most slimy" groomers, a trademark feature of their website.

Aren't some of the dangers of PJ activity only variations on the dangers of vigilantism predating the internet? It is true that people who organized themselves to mete out punishment to paedophiles in the past could be misinformed. It is also true that people could punish the "right people" – people actually guilty of grooming or worse – disproportionately. What, if anything, makes the behavior of PJ different? Part of the answer is that old fashioned crowd-sourced punishment or shaming was local, and that PJ is national and could in theory even work internationally. That is, PJ is able to mobilize a very much larger hostile audience online than local vigilantes were able to mobilize in the past. This hostile audience, what is more, can co-ordinate and prolong acts of online shaming which are difficult for those with an online presence to escape. Through online forums, local mobs and can also be reached and prompted to mete out physical punishment –but with a supposed legitimacy conferred by an organization that also co-operates with law-enforcement.

In its most typical manifestations, vigilante action is punishment – punishment by a subgroup of a community – and inflicted on misbehaving members of a community. Either that or it is hostile action by a subgroup of a community against people perceived to be intruders or interlopers. In short, vigilantism in its classic form is both communitarian and territorial – it is hostile action local to the territory of the relevant community on deviant

community members or outsiders. In other words, vigilantes can be directly affected by offenders because the life of the local community is affected. There may also be a sense in which local vigilantism is not anonymous and risks itself being seem as a violation of community norms which can attract punishment. In this respect traditional vigilantes do not enjoy impunity.

Vigilante action in this sense could be prompted by PJ in the hometowns of groomers or the premises of their employers. But the people at PJ who construct the online personas and engage the groomers are not necessarily members of the same community as the people they punish. They may live thousands of miles away and have no interactions with anyone local except through a particular chatlog. Of course, they may be co-citizens of a single national jurisdiction, but that may be too low a common denominator for the communitarian side of vigilantism to be expressed. Again, PJ digilantes may be members of a single online group of amateur sex crime police. But this, too, floats free of a particular community to which both enforcers and groomers belong and who feel the effects of both grooming and vigilantism. Merely being like-minded about child-abuse is not enough for sharing a community. Living together with those punished in the community is the important thing.

By contrast, the undercover policeman who engages with groomers online does have a link – and a morally significant link – to a community and a set of citizens via the *office* of someone who enforces its laws. The office is connected to the community through legislation that representatives of the community pass. This legislation governs action within the role of policeman or policewoman. He or she employs a set of legally constrained

techniques to carry out a preventive policing policy of a democratically legitimate legislature. This is morally far better than retaliation geared to outrage, which can differ over time and from place to place and which can be out of proportion to the harm of grooming.

A relationship that fits the PJ volunteer and the groomer better than belonging to the same community is that of being opponents in a protracted two-person online game. (Occasionally, of course, the scammer can be up against several people behind a single online persona.) Gamers do not have to share a community or much else. They need not be concerned with punishment or the guilt of the opponent. Rather, they may want to frustrate the opponent in the pursuit of his or her goals, *whatever* their moral character. This is not vigilantism, exactly, and what is wrong with it is not what is wrong with taking the law into one's own hands: what is wrong with it is not *caring* about the moral character of the opponent's goals. How the opponent's goals affect the opponent's community is also and objectionably of no interest. The gamer adopts the persona to lure the groomer, get him to reveal himself, and then prepare him for confrontation and arrest. The groomer aims at having sex with an underage partner with no adult interference. The groomer loses if he is found out or if there is no underage partner. The game of exposing groomers is lost if the PJ persona goes out of character or is caught in an inconsistency or frightens off the groomer or puts him on his guard. It is won if the groomer goes unsuspectingly to his appointment with shaming exposure. Because the moral motivation for PJ digilantism can sometimes be eclipsed entirely by simple addiction to a game in which one's opponents happen to be paedophiles, it seems to be open to charges of moral emptiness and not only charges of running too many risks of mistargeted or disproportionate punishment.

IV

I now turn to scambaiting. Zingerle[25] takes this activity to include exposure of fake organizational websites and the scripts associated with different scams, such as romance and identity scams, as well as the practice of hacking the personal computers of scammers. Although hacking is important in its own right,[26] none of the practices just listed is scambaiting, as none consists of baiting anyone. Baiting is provocation, typically aimed at making another embarrassingly angry in public, by addressing him directly. Mere exposure of scams does not satisfy this definition, even if it results in scammers getting angry. But protracted linguistic exchanges that intentionally frustrate expectations do qualify as baiting, and when they are directed at scammers and are intended to give them a taste of their own medicine before a wider audience, we have scambaiting.

Scambaiting is a response to advance fee fraud among other kinds of fraud. An example of serious fraud other than the 419 variety is the online romance scam, which consists of the use of a fake online ID to enter into a romantic relationship with someone to obtain money. Although people targeted by this scam can come from any country, there have recently been notable recorded increases in numbers from the UK, Australia, Canada and the U.S. A. The FBI's Internet Crime Complaint Center reported that there were 14,546 US victims of romance or confidence scams in 2016, a rise of over 200 per cent from 5,791 in 2014.[27]

The harm of romance scams is considerable.[28] Individuals' losses can range between £50 and £240,000[29] although the harms have been found to be a 'double hit' of financial and psychological loss.[30] According to Action Fraud, the organization in charge of publicizing and preventing fraud in the UK, nearly 10 reports per day of romance scamming were made in 2017, and embarrassment on the part of victims at being taken in by it means that this is likely to be a very considerable underestimate. Money lost to scammers in 2016 was £41 million, averaging over £11,000 per victim.[31] According to the UK national crime survey in 2016, the number of advance fee frauds in general in that year was 56,000.[32]

The forensic function of scambaiting is to disrupt advance fee fraud by frustrating particular fraudsters, and by making them more and more uncertain over time as to whether the targets they cultivate are genuine money-making opportunities or intentional time-wasters. As in the preceding section, we concentrate on an internet focal point of scambaiting practice: namely, 419 Eater.[33] Very roughly, it is to scambaiting what Perverted Justice is to paedophile-hunting. Founded in the UK in 2003 by Michael Berry –aka Shiver Metimbers— 419 Eater is a website that displays scambaiting exploits and exposes particular scammers and their methods. 419 Eater also co-ordinates and trains scambaiters to disrupt advance fee fraud. The goal of disruption can complement that of legal prosecution, and when practiced by scam victims or relations of theirs who have felt some of the ill effects of scamming as victims in the past, it can confer a therapeutic benefit.

Unlike Perverted Justice, 419 Eater is international. It targets the West Africans who dominate online advance fee fraud.[34] Again unlike Perverted Justice, which has core volunteers compiling the chatlogs and forums to comment and sometimes act against

groomers, 419 Eater seems to invite anyone to join in its direct dialogues with scammers, which it advertises on its home page as a combination of gaming and public service. The links between 419 Eater and the police are also different from those of Perverted Justice. Chatlogs of scambaiting are not usually material for prosecutions, although scambaiters may have a role in identifying scammers and even in arranging meetings e.g. the in the UK at which scammers can be interviewed and arrested by police. Some of these meetings take the form of televised sting operations intended to discomfit scammers,[35] which recalls the broadcasts made in conjunction with PJ. However, since the opprobrium attaching to fraud is much less than that associated with paedophile activity, these sting operations carry less risk for incorrectly identified scammers than for people correctly or incorrectly identified as meeting children for sex.

Scambaiting always involves (1) wasting the scammer's time by going through the motions online of being drawn into a scam, that is, by engaging in a sustained email correspondence in which one appears to be willing to pay an advance fee. Scambaiting in some forms *can* involve: (2) falsely promising in the course of (1) a large payment to a scammer on condition that they travel to a distant and sometimes dangerous location to collect it; (3) a variation on (2) in which scammed scammers are induced to post photos and videos of themselves, often adopting laughable poses and postures, as a condition of getting a payment; and (4) a variation on (2) in which scammed scammers are themselves induced to pay an advance fee for the sake of receiving an even bigger one. (2), (3) and (4) have been subject to moral criticism in both scambaiting communities and academic literature. I shall return to them. But scambaiting can and does take the form of (1) alone. This is the form I think might count as permissible digilantism.

(1) is a matter of initiating and maintaining contact with scammers and periodically undertaking and failing to send them money. It can take the form of prosaic email exchanges that keep the scambaiting targets on the hook. But it is sometimes conducted through chat logging as a low-brow art-form for a secondary audience of fellow scambaiters. Scambaiters often try to adopt handles (such as Shiver Metimbers) that would sound absurd to other people from the UK, but that scammers take at face value. Scambaiters mimic 419 scammers by finding pretexts for delaying delivery of some piece of information or money that the scammer wants, but, in addition, they try to make the pretexts sound comic to fellow scambaiters reading the exchanges in chatlogs and commenting on them on online forums. In other words, scambaiting can be a kind of intentional comedy for a secondary audience of other scambaiters and their Western online followers.

The intentions of scambaiters with respect to their primary audience – particularly online scammers – is to frustrate their plans to defraud in such a way that they slowly realize they have been manipulated and get enraged by that fact. The comedy for the secondary audience derives not only from the content of scambaiter exchanges with their targets, but from the fact that their comic content is a kind of in-joke to which only scambaiters and their Western followers are party. The fact that the scammers don't get it is part of the humour. The cultural and geographical distance between scambaiters and their targets, then, is a kind of resource for the secondary purposes of scambaiting.[36]

Compared to the scamming that it attempts to frustrate, scambaiting in the form just illustrated - i.e. (1) with comic pretensions - seems to be time-wasting, relatively harmless, deception. It seems very mild retaliation for the 419 scam or romance scam, which defrauds many people in many countries of much more money than they can afford to lose. Romance and investment scams (many also originating from West Africa) defraud people of even greater sums of money and do much psychological damage.[37]

What about the other forms of scambaiting earlier listed as morally controversial? 419 Eater has itself discontinued the collection of advance fees as part of its scamming of the scammers, even when advance fees are donated to charity. But it defends on a page of its website devoted to the ethics of scambaiting the practices it *does* permit (time-wasting and posting pictures of scammers in undignified poses).[38] The main theme of the ethics page of 419 Eater is that scammers commit serious crime and deserve much worse punishment than even the more exuberant kinds of scambaiting practice inflict. This claim is made in reply to worries from some visitors to the website that some of the photographs and videos that 419 Eater got its targets to make of themselves are demeaning or humiliating.

The fact that 419 Eater has an ethics page at all distinguishes it substantially from PJ. So does the value it places on scambaiting exchanges that work both as time-wasting and as comedy for those following them at second hand. But are the custodians of 419 Eater not too confident of occupying the moral high ground? The fact that its moral scruples are displayed on its website does not mean that it has enough of them.

The issue of whether scambaiters sometimes go too far got special attention from the well-known US National Public Radio program *This American Life* in October 2008. In that edition of the program, two scambaiters who called themselves, respectively, Yeawhatever and Professor So and So, explained a scam they turned against scammers. Posing online as officials prepared to give money to those volunteering to establish branches of a certain Western church in Africa, they attracted the interest of scammers keen to cash in and then proceeded to waste their time.

The tactic used was that of sending the scammer on what scambaiters call a 'safari': travel to, and a stay in, remote, unpleasant and even dangerous destinations, waiting for non-existent cash in large amounts to be transferred to them. The principal target of the scheme had the online name 'Adamu'. In order to collect a falsely promised $200,000, Adamu was asked to travel to Chad, at the time an active war-zone. At one point, Adamu is "asked to wear a white robe and a bright pink sash, and hold a sign with a slightly obscene message about Muhammad, this in the middle of a Muslim country." The deception of Adamu goes much further. Fictitious people who are supposed to meet him don't. Money that is supposed to reach him doesn't. He is got to move to Abeche, a very deprived and dangerous town quite near the war-torn region of Darfur. Adamu hires a driver on the understanding that soon a big money transfer will arrive through Western Union. When it doesn't, Adamu has to cope with the angry driver as well as the baiters. Pitiful-sounding emails reach the baiters, who have all along been copying their correspondence with Adamu to an online forum full of people who think Adamu is hilariously receiving his just deserts as a scammer.

When Adamu has been away from Lagos for 106 days and is at a low ebb, the baiters tell him (falsely) that his mother has died. Ira Glass, the host of *This American Life,* asks:

> Don't you think that's kind of harsh, telling somebody that their mother's dead?
>
> **Yeawhatever**
>
> Yeah, that's a little creepy. I don't know. We were talking one morning and I don't remember who came up with the idea, but it didn't sit right for a minute or two, and I thought, well, why not? So we went with it.
>
> **Jojo**
>
> But think about the irony of this. That's one thing that's kind of funny, was the response on the forum. You know, the same people that were like, oh, this is great, this is hilarious, you sent him to Chad, oh, I can't believe you've fictitiously killed his mom.
>
> **Professor So And So**
>
> Right. That's going too far.
>
> **Jojo**
>
> Sending him to Chad and the border of Darfur is fine--
>
> **Professor So And So**
>
> Which is real.
>
> **Jojo**

--but fictitiously killing his mom, oh, that's, you know, that's harsh.

JoJo is criticizing the double standards of those on the online forum, who seem to have thought that falsely informing a scammer of his mother's death crossed a line that tempting people to travel to Chad did not. For JoJo this was hypocritical. Another possible view is that ethical norms among practicing scambaiters – at least on 419 Eater – were more restrictive than JoJo realized, and defensibly so. In other words, members of the online forum justifiably shared Ira Glass's revulsion at the scambaiters' fake news.

The fact is that the treatment of Adamu does deserve criticism and does violate an acceptable ethics of scambaiting. What is more, it may deserve criticism and violate an acceptable ethics of scambaiting even from the viewpoint of scambaiters. Before we develop this claim, however, let us reflect on what JoJo and Professor Whatever did *not* do. They did not exact advance fees for themselves as part of their deception about the church subsidy. They did not gain financially from Adamu at all. They admittedly lied to him, broke promises to him, casually invited him to waste time and money, and put him in danger. This reflects the fact that their purpose was to punish an advance fee fraudster in such a way that he would experience some of what the victims of the 419 scam experience. To the extent that Adamu's experiences were not equivalent to, but worse than, those of a standard scam victim, the conduct of the scambait is questionable by reference to the purpose of the scambaiters themselves. Adamu's experiences *did* seem worse. Adamu was given incentives to go to war zones and put his life at risk. Again, falsely informing Adamu of his mother's death seems wrong even when judged by scambaiter standards, because it does not have a counterpart in the standard experience of the scam victim. Moreover, it is

unnecessarily personal and occurs after a long period in which Adamu has already experienced lots of unpleasantness.

But to criticize the scambaiters for the excesses of their punishment in this case is not necessarily to criticize the very idea of their punishing scammers by wasting their time through email and "safaris" that do *not* put them in harm's way. Many scammers in West Africa operate with what amounts to impunity. It is often open to them to bribe their way out of trouble. There are many potential new recruits to scamming waiting to replace any who are imprisoned. Scambaiting activity raises the probability that scamming activity will be ineffective. It makes scammers more uncertain whether, when they make contact with a foreigner online, they are dealing with a promising mark or a digilante. It also raises the money costs of scamming to those who are taken in by scambaiters and have to travel or pay for costly couriers.

Compared to the ill effects on those who are the targets of paedophile-hunting, the ill effects of having one's time wasted through email correspondence or undertaking unnecessary but safe travel are mild. Nor are there high costs of online exposure as a scammer through photographs in the trophy room. First, it appears not to be dishonorable in Nigeria or Ghana to make money from scamming if one is young and poor.[39] On the contrary, university students who operate as scammers are admired by their peers.[40] Online scammers even have cult Youtube followings,[41] in much the way some young gangsters have in the US or UK. Second, local prosecutions are made difficult by the sheer volume of scamming, the ubiquity of corruption, and the difficulty of tying online to physical identities. So scambaiting adds to the cost of scamming without necessarily harming the harmers significantly.

I do not claim that scambaiting in even its mildest form of low-humour correspondence without safaris is *absolutely* harmless. The fact that scammers are sometimes unaware of the fun being made of them by Shiver Metimbers does not mean that they would not feel humiliated if they *were* made aware of it. And scambaiters themselves sometimes feel uneasy with the gallery of ridiculous poses adopted by scambaiting targets and exhibited as trophies on the 419 Eater site. These images may be objectionable just because the cultural distance between scambaiters and their targets keeps the targets from knowing that their images are being used for public ridicule, and because cultural difference in this case may seem to feed impressions in the scambaiting community of cultural superiority over scammers.

Nakamura (2014) has gone much further than I would in condemning the 419-Eater trophy room. After discussing some admittedly disturbing examples of photographs from that source that have become memes, she writes:

> The surreal, bizarre, and racist-baroque photographs seen in the 'Trophy Room' are an eloquent testament to the power of the internet to victimize and to offend. However, it is not really the digital network that has produced a new racist aesthetic system – the set of conventions seen in scambaiters' trophies visualize an exercise in racial power for its own sake.[42]

This seems to me to be an exaggeration for several reasons. First, the images she makes the most of do not seem to me to be representative of those in the Trophy Room. Typical images are of unsmiling, well-dressed people unenthusiastically holding up signs with low-humour messages demanded in written correspondence from a scambaiter. These images

seem to me to show people who are doing what the scambaiters require through gritted teeth --for the money. Second, the claim of exercise of racial power for its own sake seems to airbrush away the harm of scams coming from Nigeria and Ghana, harm that much more obviously motivates scambaiters than racism. Third, relatively few of the 410 Eaters provide material for the trophy room. This means that sweeping charges of racism against scambaiters in general based on trophy photographs are questionable. Fourth, as Nakamura herself admits, it is perfectly possible that the subjects of the photos are, as she puts it, "in on the joke".[43] This limits their victimization.

There is nevertheless a general moral problem with scambaiting that we can broach through the case of Adamu discussed earlier. The problem can be put by asking how Hey Whatever and Professor So and So *knew* that Adamu was a scammer. Clearly if they did not know, they ran the risk of severely wronging Adamu by sending him off in search of a non-existent $200,000. On the other hand, if they did know that he was a scammer, how much did they know about the harm that Adamu had in the past inflicted in that role? If the scambaiters knew nothing about Adamu's past actions in particular but would have asked *anyone* they took to be a scammer on the basis of impressions alone to visit a war-zone, then they ran the risk of meting out punishment significantly out of proportion to the misdeeds of a particular scammer. Meting out the same severe punishment to any old scammer is as objectionable as punishing a mass murder the same as a one-off murder. The fact that the punishment is, in addition, meted out ad hoc and on a whim – as in the case of falsely informing Adamu that his mother had died – illustrates disproportionate punishment contributed by bad or incomplete background information on scammers. On the other hand, it is not so clear that scambaiting has to involve safaris, or that it typically does, and

the fact that at least some scambaiters are against scambaiting in that form shows that the norm of avoiding safaris Is not merely utopian. The core activity of long and drawn out email exchanges – with or without comic flourishes or safaris – seems to be the typical activity.

Professor So and So and his accomplices in scambaiting may have treated Adamu not as an individual with a record of misdeeds he was responsible for, but as someone who represents scammers in general and deserves a punishment fitting the typical scammer. This homogenization is of course morally objectionable, and, to allude to a suggestion made earlier, it is reminiscent of online gaming; where the opponents are often all look-alikes. There is a counterpart of this homogenization in the case of scammers and scam victims alike. The 419 scam consists of mass e-mailings to addresses of people in a mostly undifferentiated rich global North and West who (in scammers' eyes but on no particular evidence) can all afford financial losses. What is more, those who respond are easily stereotyped as gullible, greedy and unscrupulous people who deserve their losses. Sometimes, in addition, they are stereotyped as people from the countries that colonized Africa and whose inhabitants profited from the oppression of Africans. The stereotypes are sometimes wrong, since some people targeted come from countries (e.g. Canada and Australia) with no role in African colonization. Both kinds of homogenization encourage inattention – on the part of scammers and scambaiters alike – to the magnitude of harms visited on particular people. But at least the stereotypes are misused on both sides.

It might be thought that the wrongdoing of scammers from West Africa is partly explained and mitigated by global inequalities that West Africans are not allowed to alleviate through migration, and by local inequalities that are hard to combat. What else are they to do to earn a living? Western African scammers often start out as impoverished young people

whose opportunities are reduced by local corruption, by the concentration of power and wealth in a small local elite, and by intergenerational relations in which the relatively young are at a disadvantage.[44] That, however, does not justify resort to scamming nearly as much as it supports comprehensive political reform and the opening of opportunity locally.

It is perfectly possible that Western governments have a big role to play in encouraging such reform through aid programmes and police co-operation, and it is perfectly possible that the colonial past of e.g. the UK creates a weighty obligation to assume that role. But it is flatly false to say that in the meantime all the inhabitants of the ex-colonizing countries, or all the inhabitants of rich jurisdictions, or even all of the rich inhabitants of the rich jurisdictions, are fair game for scammers. Scamming is highly harmful activity undeniably motivated in most cases by personal gain and carried out under assumed names and with many precautions taken against police action. In short, it bears may of the hallmarks of a typical criminal enterprise. It is hardly an exercise in global ethics. On the other hand, there are global ethics issues --as well as domestic ethics and intergenerational ethics issues-- behind the relative poverty of African and other countries in which scamming is carried out as organized crime.

Conclusion.

Not all forms of digilantism are morally on a par, and not all carry the risks that typify traditional vigilantism. I have suggested that in at least one of its actual forms, scambaiting is a relatively harmless form of digilantism. It does not physically injure its targets, and the evidence that it humiliates them or replays colonializing behaviour seems overdrawn.

Instead digilantism often wastes the time of scammers, prevents fresh victimization by those whose time is taken up, and makes scammers more uncertain that they will not be taken in the next time they identify a target. These effects seem to make scamming harder and less profitable at the same time as they raise the risks for scammers of being scammed themselves, with, in their case, no financial losses. It is true that there is little to stop scambaiters resorting to more extreme means of teaching scammers a lesson. The point being made here is that non-extreme means may be effective, and that existing norms on at least the most prominent scambaiting site support the use of non-extreme means.

Other forms of digilantism produce much greater harm and much greater collateral damage. Paedophile hunting in many of its most familiar forms runs great risks of violent retaliation against real and falsely presumed groomers and child rapists alike. The consequences of false accusations are much more likely than in scambaiting to be serious, including, at times, fatal. The ease of becoming an online digilante, the impunity conferred by anonymity, and the weak claim of digilantes to belong to the communities they police all count against digilante activity the more associated it is with violence. But some digilantism can be barbed without being violent. This is what distinguishes scambaiting from other varieties of digilantism.

Notes

1. Research for this paper was supported by the UK Engineering and Physical Science Research Council Grant No. EP/N028112/1 ("Detecting and Preventing Mass-Market Fraud").

2. One of the earliest examples of digilantism was directed against Intel for manufacturing defective computer chips. See Badaracco, "The Internet, Intel and the Vigilante Stakeholder"

3. Ronson, *So You've Been Publicly Shamed?*

4. Hardaker, "I Refuse to Respond to This Obvious Troll"; Hardaker, "Real Men Don't Hate Women"; Phillips, *This is Why We Can't Have Nice Things*.

5. Woolford and Thomas, "Exception and Deputization Under Today's NDP".

6. DIY Policing http://media4sec.eu/workshops/diy/

7. Daily Mirror 18 September 2018 https://www.mirror.co.uk/news/politics/80000-british-paedophiles-pose-sexual-13181652

8. Wilkinson, "Putting Traditional Values into Practice."

9. Kosseff, "The Hazards of Cyber-Vigilantism."

10. Jane, "Online Misogyny and Feminist Digilantism."; Jane, "Flaming? What flaming?"; Jane, "Your a Ugly, Whorish, Slut."; Jane, "Back to the Kitchen, Cunt."

11. See for example, Citron, *Hatecrimes in Cyberspace* and Ronson, *So You've Been Publicly Shamed?*

12. Laidlaw, "Online Shaming and the Right to Privacy."

13. Levmore and Nussbaum, *The Offensive Internet.*

14. Trottier, "Digilantism as Weaponization of Visibilty."

15. There is relatively little definitional work on vigilantism and quite a lot of disagreement over its necessary conditions. See for example: Rosenbaum and Sederberg, *Vigilante Politics*; Johnston, "What is vigilantism?"; and Dumsday, "On Cheering Charles Bronson." A certain amount of distortion has been produced by concentration in some literature on a solo vigilante figure, such as the cinema character Charles Bronson. Vigilantism is sometimes connected with action against behaviour perceived as violating local norms even if not laws (see Rosenbaum and Sederberg *Ibid*.)

16. Paedophile-hunting groups such as The Hunted One and Dark Justice post videos of their confrontations with identified groomers on Youtube: https://www.youtube.com/channel/UCA86yT9Xh_w1pVa4BadXPZQ; https://www.youtube.com/user/Dark1Justice

17. https://darkjustice.co.uk/

18. The Guardian 8 April 2017 https://www.theguardian.com/society/2017/apr/08/judge-rules-paedophile-hunters-can-continue-posing-as-children-online

19. https://www.cps.gov.uk/legal-guidance/vigilantes-internet-cases-involving-child-sexual-abuse

20. http://www.perverted-justice.com/?archive=aGreatGuy

21. 'To Catch a Predator: the new American witch-hunt' *Rolling Stone* July 2007 http://www.rollingstone.com/tv/features/the-new-american-witch-hunt-20070809. It is difficult to find authoritative sources on either Perverted Justice or 'To Catch a Predator'. Apart from the Wikipedia and RationalWiki articles on both, the Rolling Stone piece is perhaps the most revealing.

22. Sorell, "Online Grooming and Preventive Justice."

23. Information in this paragraph is based on conversations between the author and members of a UK police force.

24. “No one is home at this house on the Jersey Shore — no one, that is, except a very cute and horny fourteen-year-old. Her parents went to Atlantic City for the weekend, she is telling guys online, and she wants to get laid. Dozens of men are now making their way to the house, hoping to get lucky with an underage kid. One man rings Casey, the hired decoy who is impersonating a 14-year old for the occasion, and expresses second thoughts about meeting:

> Casey gabs to potential predators on the phone. "Come on over, we're not going to get caught," she says. "If we got caught, I would get into trouble, and everybody would call me a slut, and I don't want that, either. I'll *pay* for your gas. It's no big deal, trust me. My dad gave me plenty of money for the weekend." When the guy fails to take the bait, her voice rises in pitch. "OK, fine, whatever, lame. L-A-M-E. You're being a baby. I told you I've done it a million times!"

Although the actress quoted is not the same person as the PJ operative who has constructed the persona of the 14 year old and maintained the relationship with each groomer now on his way to New Jersey, all the groomers believe that they are meeting their online conversation partners. One of the men who arrives is only just out of his teens himself, and he too, had to be argued out of his reluctance to meet an under-age girl and get prosecuted.

> Everyone [in the TCP crew] turns their attention to the camera following the Impala as it disgorges Ikeman, a.k.a. John Donnelly, a handsome twenty-one-year-old who is wearing a striped sweatshirt and a look that's equal parts sexual anticipation and terror. Casey runs outside to meet him, taking a seat in a chair on the beach. He approaches slowly.
>
> "Where are the wine coolers?" she asks.
>
> "I was going to get them after I met you because I was so paranoid," Donnelly says, looking around. "Man, I was just worried about this shit because I never met anyone under eighteen." He scrutinizes a couple passing by. "I guess there are no cops around, so it's cool."
>
> "Yeah," says Casey, smiling. "You can see there's no one here."
>
> He rubs his head. "I'm just worried that it's some crazy scheme," he says. "It's just like what you see on the news."

These are the last words he utters before being confronted by Chris Hansen, the host of 'To Catch a Predator'.

25. Zingerle, "Scambaiters, Human Flesh Search Engine, Perverted justice, and Internet Haganah: Villains." Also by Zingerle, "Towards a Categorization of Scambaiting Strategies Against Online Advance Fee Fraud.". See also Tuovinen and Roning, "Baits and Beatings".

26. Jordan, *Internet, Society and Culture;* Jordan and Taylor, *Hacktivism and Cyberwars*

27. USA Today November 29 2017 https://eu.usatoday.com/story/money/2017/07/20/fbi-says-internet-romance-scams-rise/485311001/

28. See e.g. Conway et. al. “Scamming and its Effect on Vulnerable Individuals.” See also Sorell and Whitty, “Online Romance Scams and Victimhood.”

29. Whitty, “Anatomy of the Online Dating Romance Scam.”

30. Whitty and Buchanan, “The Online Dating Romance Scam”

31. https://www.actionfraud.police.uk/news/victims-lost-41-million-to-romance-fraud-in-2017

32. Office of National Statistics “Overview of Fraud and Computer Misuse Statistics for England and Wales.”

33. http://www.419eater.com/

34. These are sometimes known as “Yahooboys” after the internet search engine. For the role that local politics and corruption plays in generating Yahooboy culture, see Adenirin, “The Internet and Emergence of Yahooboys Sub-Culture in Nigeria.”

35. https://www.youtube.com/watch?v=F4Qpo_d0MOc

36. As an example of the genre I choose an excerpt from a scambaiting correspondence due to Shiver Metimbers directed at a Nigerian “businessman” who believes he is eligible for funding in return for submitting two samples of artwork by post to a UK address. The art is duly submitted, and then claimed by the scambaiter to have arrived damaged. In an undamaged state, the scambaiter (falsely) claims, the samples would have been worth around £40,000. There then follows a long exchange about returning the damaged art work, which itself is said to have been lost by the courier. The exchange is conducted by the scambaiter using the name Derek Trotter, borrowed from the TV character Del Trotter, a fictional London dealer in stolen and fraudulent goods in the (now long defunct) BBC TV series *Only Fools and Horses*. The receipt from the courier is signed ‘Charles Manson’. The covering letter reads as follows:

Dear Mr. Ofuonyeadi,

Thank you for your patience.

I have bad news and good news for you. The bad news is that Tribble Postal Systems have now admitted to me that they have lost your artwork somewhere in transit (not sure where that is, but it sounds like a place I don't want to be). Anyway, I spoke with the head honcho at Tribble HQ and after a heated telephone conversation the good news is that they have agreed to pay compensation for the loss of the artwork.

I do apologise for all the delay Mr. Ofuonyeadi but I hope you will understand that this is not my fault but those lazy arsed vagabonds at Tribble Postal Systems.

After some consultation they have agreed to pay my full compensation claim of UK £38,774 (US $68,760), and this morning I received a letter and cheque for the full amount, which I will cash later this afternoon.

For your records I have attached a copy of the letter and of course a scan of the cheque. Once again I apologise for the rather rough appearance of the letter but Bert the hamster got his paws on it whilst I left it at the dining room table on one of my many visits to the toilet (I have been suffering from food poisoning after eating a very badly cooked ratburger). I'll swing for that hamster one of these days, you mark my words.

Anyway, I hope that you will be happy with the outcome and I shall await your reply at your earliest convenience.

Sincerely,

Derek Trotter

Trotters Fine Arts

www.deltrotter.co.uk

37. http://www.bbc.co.uk/news/uk-38678089

38. http://www.419eater.com/html/ethics.htm

39. Burrell, *Invisible Users.* In chapter three Burrel argues that many of the Yahoo boys in Ghana are caught between a controlling local older generation,which severely limits their local economic and social opportunities, and an international community whose prejudices against Africans limit the possibilities of access via online friendship to the rich, Western world. According to Burrell Ghanaians experience pretty consistent digital "shunning". These circumstances force them into online misrepresentation. In addition, Ghanaian customs of asking for money from friends or loved ones (*Ibid*. p.62) are easily misunderstood by foreigners. Even if all of this is correct, it fails to justify elaborate fraud and its harms. Burrell seems to describe romance scamming tendentiously as "flexible self-presentation for the purpose of persuasion" (*Ibid*. p.72) when what it is, is sustained deception for the purpose of making money.

40. Ojedokun and Eraye, "Socioeconomic Lifestyles of the Yahoo-Boys"

41. https://www.youtube.com/watch?v=xblrJW4gttg

42. Nakamura, "I WILL DO EVERYthing That Am Asked," 270.

43. Nakamura *Ibid.* p.271. Again, as Burrell notes on p.75 of *Invisible Users* the distortion of the other goes in both directions: "As Africans are typified in the West by poverty-stricken famine victims on the television, Westerners are typified by wealthy celebrities. Whereas Africans are needy, Westerners are greedy. This mutually agreed-on asymmetry is exaggerated into mutual misunderstanding."

44. Burrell, *Invisible Users.*

Bibliography

Adenirin, Adebusuyi I. "The Internet and Emergence of Yahooboys Sub-Culture in Nigeria." *International Journal of Cyber Criminology* 2, No. 2 (2008): 368–381.

Badaracco, Joseph, L. "The Internet, Intel and the Vigilante Stakeholder." *Business Ethics* 6, No. 1 (1997): 18–29.

Bland, Lucy. 'Purifying' the public world: feminist vigilantes in late Victorian England", *Women's History Review* 1 (1992) 397-412

Burrell, Jenna. *Invisible Users: Youth in the Internet Cafes of Urban Ghana*, Cambridge MA: MIT Press. 2012.

Citron, Danielle. *Hatecrimes in Cyberspace.* Cambridge, MA: Harvard University Press, 2014.

Conway, L., Thurley, D., and Edmonds, T. "Scamming and its Effect on Vulnerable Individuals" UK House of Commons briefing paper Number CBP-07691, 6 September 2016. https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7691#fullreport.

Dumsday, Travis. “On Cheering Charles Bronson: The Ethics of Vigilantism.” *The Southern Journal of Philosophy* 47, No.1 (2009): 49–67.

Fezzani, Nadia. *Real Life Super Heroes.* Toronto: Dundurn, 2016.

Hardaker, Claire. “'I Refuse to Respond to This Obvious Troll': An Overview of Responses to (Perceived) Trolling.” *Corpora* 10, No.2 (2015): 201-229.

Hardaker, Claire. ‘“Real men don't hate women’: Twitter Rape Threats and Group Identity.” *Journal of Pragmatics* 91 (2016): 80-93.

Jane, Emma, A. “’Back to the Kitchen, Cunt’: Speaking the Unspeakable about Online Misogyny’ *Continuum* 28, No. 4 (2014): 558–570.

Jane, Emma, A. “Flaming? What Flaming? The Pitfalls and Potentials of Researching Online Hostility.” *Ethics and Information Technology* 17, No.1 (2015): 65–87.

Jane, Emma, A. “Online Misogyny and Feminist Digilantism.” *Continuum* 30, No. 3 (2016): 284-297.

Jane, Emma, A. “Your a Ugly, Whorish, Slut.” *Feminist Media Studies* 14, No. 4 (2014): 531–546.

Johnston, Les. ‘What is Vigilantism? *British Journal of Criminology* 36, No. 2 (1996): 220–236.

Jordan, Tim. *Internet, Society and Culture: Communicative Practices Before and After the Internet*. London: Bloomsbury, 2014.

Jordan, Tim and Taylor, Paul. *Hacktivism and Cyberwars: Rebels with a Cause?* London: Routledge, 2004.

Juliano, Stephanie. “Superheroes, Bandits, and Cyber-nerds: Exploring the History and Contemporary Development of the Vigilante” *Journal of International Commercial Law and Technology* 7, No.1 (2012): 44–64

Kosseff, Jeff, "The hazards of cyber-vigilantism." *Computer Law and Security Review* 32 (2016): 642–649.

Laidlaw, Emily, B. "Online Shaming and the Right to Privacy." *Laws* 6, No. 3 (2017): 1-26.

Levmore, Saul and Nussbaum, M. *The Offensive Internet.* Cambridge, MA: Harvard University Press, 2012.

Nakamura, Lisa. "'I WILL DO EVERYthing That Am Asked': Scambaiting, Digital Show-Space, and the Racial Violence of Social Media" *Journal of Visual Culture* 13, No.3 (2014): 257-274.

Office of National Statistics (UK) "Overview of fraud and computer misuse statistics for England and Wales." https://bit.ly/2EcY0Os

Obert, Jonathan, *The Six-Shooter State*. Cambridge: Cambridge University Press, 2018.

Ojedokun, Usman Adekunle and Eraye, Michael Christopher. "Socioeconomic Lifestyles of the Yahoo-Boys: A Study of Perceptions of University Students in Nigeria." *International Journal of Cyber Criminology* 6, No. 2 (2012): 1001-1013.

Phillips, Whitney. *This is Why We Can't Have Nice Things.* Cambridge MA: MIT Press, 2015.

Ronson, Jon. *So You've Been Publicly Shamed?* London: Riverhead, 2015.

Rosenbaum, H. Jon and Sederberg, Peter. *Vigilante Politics*. Philadelphia: University of Pennsylvania Press, 1976.

Sorell, Tom and Whitty, Monica. "Online Romance Scams and Victimhood." *Security Journal* Jan 2019. https://link.springer.com/article/10.1057/s41284-019-00166-w

Sorell, Tom. "Online Grooming and Preventive Justice." *Criminal Law and Philosophy* 11, No.4 (2017): 705–724.

Trottier, Daniel "Digilantism as Weaponization of Visibility." *Philosophy and Technology* 30, No. 1 (2016): 55-72.

Tuovinen, Laurie and Roning, Juha. “Baits and Beatings: Vigilante Justice in Virtual Communities.’ *Proceedings of CEPE 2007. The 7th International Conference of Computer Ethics: Philosophical Enquiry* (2007): 397-405.

Whitty, Monica and Buchanan, Tom. “The Online Dating Romance Scam: The Psychological Impact on Victims – Both Financial and Non-Financial.” *Criminology & Criminal Justice* 16, No.2 (2016): 176-194.

Whitty, Monica. “Anatomy of the Online Dating Romance Scam.” *Security Journal* 28 (2015): 443-455.

Wilkinson, Cai. “Putting Traditional Values Into Practice: Russia’s Anti-Gay Laws.” *Russian Analytical Digest* 138 (2013): 5-7.

Woolford, Andrew and J. Thomas. “Exception and Deputization Under Today’s NDP: Neo-Liberalism, The Third Way, and Crime Control in Manitoba.” *Canadian Journal of Law and Society* 26, No. 1 (2011): 113–131.

Zingerle, Andreas. ‘Scambaiters, Human Flesh Search Engine, Perverted justice, and Internet Haganah: Villains, Avengers, or Saviors on the Internet?’ file:///Scambaiters_Human_Flesh_Search_Engine_Pe%20(2).pdf.

Zingerle, Andreas. “Towards a Categorization of Scambaiting Strategies Against Online Advance Fee Fraud.” *International Journal of Art, Culture and Design Technologies* 4, No.2 (2014): 39–50.